(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051456 A3

(51) International Patent Classification[7]: G06F 7/72

(21) International Application Number: PCT/IB2003/005095

(22) International Filing Date: 11 November 2003 (11.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0227793.7 29 November 2002 (29.11.2002) GB

(71) Applicant (*for all designated States except US*): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): HUBERT, Gerardus, T., M. [NL/NL]; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(74) Agent: TURNER, Richard, C.; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

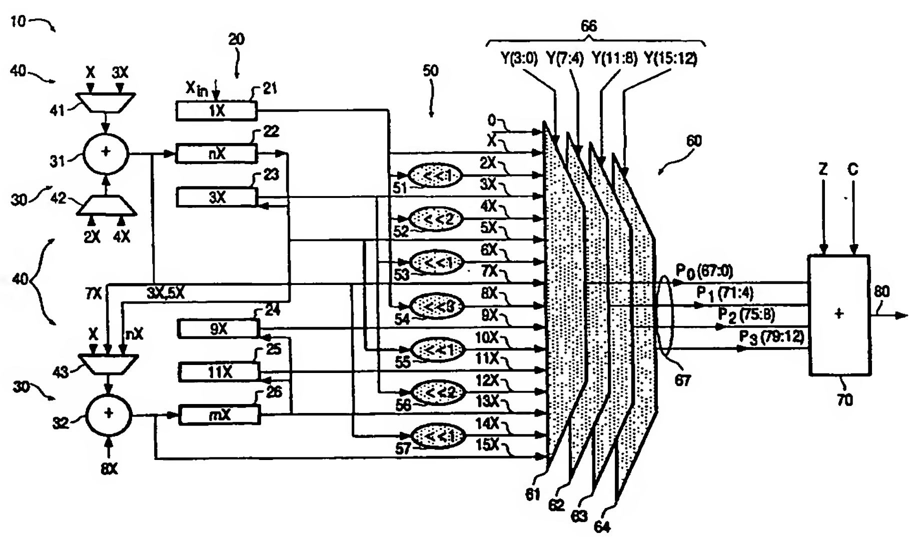
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,*

[Continued on next page]

(54) Title: MULTIPLIER WITH LOOK UP TABLES



(57) Abstract: A method of performing modular multiplication of integers X and Y to produce a result R, where R = X.Y mod N, in a multiplication engine. X is fragmented into a first plurality of words xn each having a first predetermined number of bits, k and Y is fragmented into a second plurality of words y_n each having a second predetermined number of bits, m. Multiples of a word x_n of X are derived in a pre-calculation circuit and subsequently used to derive products of the word x_n of X with each of the plurality of words y_n of Y. An intermediate result R_j is calculated as a cumulating sum derived from said pre-calculated multiples and the steps repeated for each successive word of X so as to generate successive intermediate results, R_j, for each of the first plurality of words x_n. The final result, R is obtained from the last of the intermediate results R_{n-1}.

WO 2004/051456 A3

RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 16 December 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/05095

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 864 529 A (SHAH IMRAN A ET AL) 5 September 1989 (1989-09-05)	15-17
Y	column 1, line 52 - column 2, line 11 abstract column 3, line 16 - column 5, line 44 figures 4,5	1-14,18, 19
Y	WO 02/03608 A (KOC CETIN K ; SAVAS ERKAY (US); OREGON STATE (US); YANIK TUGRUL (US)) 10 January 2002 (2002-01-10) abstract page 3, line 12 - page 4, line 27 page 10, line 30 - page 14, line 7	1-14,18, 19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 September 2004	22/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Form PCT/ISA/210 (second sheet) (January 2004)

International Application No
PCT/GB 03/05095

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 121 431 A (WIENER MICHAEL J) 9 June 1992 (1992-06-09) abstract column 1, line 45 - column 2, line 52 figures 1,2	1-19

INTERNATIONAL SEARCH REPORT

In[illegible]al Application No
P[illegible]B 03/05095

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 4864529	A	05-09-1989	NONE			
WO 0203608	A	10-01-2002	AU	7365301	A	14-01-2002
			WO	0203608	A1	10-01-2002
			US	2002059353	A1	16-05-2002
US 5121431	A	09-06-1992	CA	2045385	A1	03-01-1992